Written Statement of

Donald (Andy) Purdy, Jr.

Director (Acting), National Cyber Security Division

Information Analysis and Infrastructure Protection Directorate

U.S. Department of Homeland Security

Homeland Security Committee

United States House of Representatives

October 18, 2005

Good morning Chairman King and distinguished members of the Committee. My name is Andy Purdy, and I am the Acting Director of the Department of Homeland Security's National Cyber Security Division (NCSD). I am delighted to appear before you today to share with you the work of the NCSD to address one of the significant threats to our cyberspace and critical infrastructure – industrial control systems.

In my testimony today, I will provide an overview of NCSD's mission and goals, priorities, and partnerships, with a particular focus on our Control Systems Security Program. The Control Systems Security Program addresses the cyber security of industrial control systems that run the operational processes within the nation's critical infrastructure.

DHS and Critical Infrastructure Protection

Over the course of the past several months Secretary Chertoff conducted a systematic evaluation of the Department's operations. On July 13th, Secretary Chertoff announced the results of that evaluation and outlined his six point agenda for the path ahead for the Department. As part of this agenda, the Secretary announced several Departmental organizational changes. Among these was the creation of a new Preparedness Directorate which would house a newly created office of the Assistant Secretary for Cyber Security and Telecommunications. According to Secretary Chertoff, "Securing our cyber systems is critical not only to ensure a way of life to which we've grown accustomed, but more importantly to protect the vast infrastructure these systems support and operate."

Currently, the Office of Infrastructure Protection (IP), located within the Information Analysis and Infrastructure Protection (IAIP) Directorate, is responsible for all critical infrastructure and key resource protection. The Office of Infrastructure Protection has four component divisions: (1) the Infrastructure Coordination Division (ICD), (2) the Protective Security Division (PSD), (3) the National Communications System (NCS), and (4) the National Cyber Security Division (NCSD).

In December 2003, President Bush issued Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection (HSPD-7), which established a national

policy for federal departments and agencies to identify and prioritize United States critical infrastructure and key resources and to protect them from terrorist attacks. Among other things, HSPD-7 identified seventeen (17)[1] critical infrastructure and key resource sectors and assigned responsibility for each to a Sector Specific Agency (SSA), with DHS serving as the overall program coordinator.

Additionally, HSPD-7 set forth how DHS should address critical infrastructure protection, including development of a "summary of activities to be undertaken in order to: define and prioritize, reduce the vulnerability of, and coordinate the protection of critical infrastructure and key resources."[2] To meet this mandate, IP developed the interim National Infrastructure Protection Plan (NIPP), a plan that is to serve as the guide for addressing critical infrastructure and key resource protection. It sets forth a risk management framework for public and private sector stakeholders to work together to identify, prioritize, and conduct vulnerability assessments of critical assets and key resources in each sector. It also includes the identification of interdependencies of critical assets and key resources both within and across the sectors as well as providing priority protective measures that owners and operators of such assets should undertake to secure them. Recognizing that more that 85 percent of the critical infrastructure is owned and operated by the private sector and that the development of public-private partnership is paramount to securing our nation's assets, private sector-led Sector Coordinating Councils (SCCs) are being established to work with their appropriate SSA via Government Coordinating Councils (GCC), which represent the government agencies that have a role in protecting the respective sectors.

Currently, the Office of Infrastructure Protection is finalizing the NIPP and it is expected to be released later this year. This finalized document will refine the public-private partnership model and a process for protecting our critical infrastructures from physical or cyber attack or natural disasters.

DHS and Cyber Security

In June 2003, in response to the President's *National Strategy to Secure Cyberspace*, the Department of Homeland Security created the NCSD as a national focal point for cyber security. The national strategy established the following five national priorities for securing cyberspace:

Priority I:	A National Cyberspace Security Response System
Priority II:	A National Cyberspace Security Threat and Vulnerability Reduction Program
Priority III:	A National Cyberspace Security Awareness and Training Program
Priority IV:	Securing Government's Cyberspace
Priority V:	National Security and International Cyberspace Security Cooperation

[1]The NIPP identifies the following Critical Infrastructure Sectors and Key Resources: Food and Agriculture; Public Health and Healthcare; Drinking Water and Wastewater; Energy; Banking and Finance; National Monuments and Icons; Defense Industrial Base; Information Technology; Telecommunications; Chemical; Transportation Systems; Emergency Services; Postal and Shipping; Dams; Government Facilities; Commercial Facilities; Nuclear Reactors, Materials, and Waste.

[2] Homeland Security Presidential Directive 7, December 17, 2003; http://www.whitehouse.gov/news/releases/2003/12/20031217-5.html.

Given today's interconnected environment and DHS's integrated risk-based approach to critical infrastructure protection, NCSD's mission is to work collaboratively with public, private, and international entities to secure cyberspace and America's cyber assets. To meet that mission, NCSD developed a Strategic Plan that establishes a set of goals with specific objectives for each goal, and milestones associated with each objective. The Strategic Plan goals, which are closely aligned with the Strategy, HSPD-7, the NIPP, and the Cyber Annex to the recently announced National Response Plan, are as follows:

1. Establish a National Cyberspace Response System to prevent, detect, respond to, and reconstitute rapidly after cyber incidents;
2. Work with public and private sector representatives to reduce vulnerabilities and minimize severity of cyber attacks;
3. Promote a comprehensive awareness plan to empower all Americans to secure their own parts of cyberspace;
4. Foster adequate training and education programs to support the Nation's cyber security needs;
5. Coordinate with the intelligence and law enforcement communities to identify and reduce threats to cyberspace; and
6. Build a world class organization that aggressively advances its cyber security mission and goals in partnership with its public and private stakeholders.

To meet these goals, NCSD is organized into four operating branches to address the various aspects of the risk management structure: (1) U.S. Computer Emergency Readiness Team (US-CERT) Operations to manage the 24x7 threat watch, warning, and response capability that can identify emerging threats and vulnerabilities and coordinate responses to major cyber incidents; (2) Strategic Initiatives to manage activities to advance cyber security in critical infrastructure protection, control systems security, software development, training and education, exercises, and standards and best practices; (3) Outreach and Awareness to manage outreach, cyber security awareness, and partnership efforts to disseminate information to key constituencies and build collaborative actions with key stakeholders; and (4) Law Enforcement and Intelligence to coordinate with and share information between these communities and NCSD's other constituents in the private sector, public sector, academia, and others, and also to coordinate DHS efforts within interagency response and mitigation of cyber security incidents. Together, these branches make up NCSD's framework to address the cyber security challenges across our key stakeholder groups and build communications, collaboration, and awareness to further our collective capabilities to detect, recognize, attribute, respond to, mitigate, and reconstitute after cyber attacks.

The Strategy, HSPD-7, and the interim NIPP provide NCSD with a clear operating mission and national coordination responsibility. To carry out this mission and its related responsibilities, NCSD has identified two overarching priorities: to build an effective national cyberspace response system and to implement a cyber risk management program for critical infrastructure protection. Our focus on these two priorities and related programs addresses the overarching NIPP Risk Management

methodology and establishes the framework for securing cyberspace today and a foundation for addressing cyber security for the future.

Within the second priority, in addition to fulfilling our NIPP role as the Sector Specific Agency for the Information Technology (IT) Sector and providing cross-sector cyber security guidance to all sectors, NCSD undertakes a cyber risk mitigation approach focused on three key areas. These include the Internet Disruption Working Group, the Software Assurance Program, and the Control Systems Security Program.

NCSD and Control Systems Cyber Security

The interdependency between physical and cyber infrastructures is hardly more acute than in the use of control systems as integral operating components by many of our critical infrastructures. "Control Systems" is a generic term applied to hardware, firmware, communications, and software used to perform vital monitoring and controlling functions of sensitive processes and enable automation of physical systems. Specific types of control systems include Supervisory Control and Data Acquisition (SCADA) systems, Process Control Systems (PCS), and Distributed Control Systems (DCS).

Examples of the critical infrastructure processes and functions that control systems monitor and control include energy transmission and distribution, pipelines, water and pumping stations, telecommunications, chemical processing, pharmaceutical production, rail and light rail, manufacturing, and food production. Increasingly, these control systems are implemented with remote access and connections to open networks such as corporate intranets and the Internet. Older control systems that operated with manual components, vacuum actuators, and proprietary software are rapidly being upgraded with modern computer systems. These sophisticated IT tools are making our critical infrastructure assets more automated, more productive, more efficient, and more innovative, but they also may expose many of those physical assets to physical consequences from new, cyber-related threats and vulnerabilities.

Control systems represent an attractive target for malicious actors for several reasons. First, they provide a possible avenue for inflicting physical, environmental, or economic harm to the nation from a distance. Second, relatively mature attacking tools have been developed and are available on the Internet. Finally, these tools can be used with little technical expertise to attack control systems that are accessible from the Internet.

To assure immediate attention is directed to protect these systems, NCSD established the Control Systems Security Program to coordinate efforts among federal, state, and local governments, as well as control system owners, operators, and vendors to improve control system security within and across all critical infrastructure sectors.

The Program incorporates five highly integrated goals to address the issues and challenges associated with control systems security.

1. Coordinate control system incident management, provide timely situational awareness information for control systems, assess control system vulnerabilities, encourage voluntary

reporting, and manage control system vulnerability and threat reduction activities by enhancing the US-CERT's capabilities for control systems security;

2. Reduce control system cyber vulnerabilities in Critical Infrastructure by establishing a proactive environment for risk reduction and security assessments, to evaluate systems, and to work with control systems owner/operators and vendors to resolve vulnerabilities;
3. Bridge industry and governmental efforts through participation in working groups, standards development bodies, and user conferences to build cooperative and trusted relationships and enhance control systems security efforts;
4. Develop control systems security awareness and create a self-sustaining security culture within the control systems community; and
5. Make strategic recommendations as to the funding, development, and testing of next-generation secure control systems and security products.

Goal 1 - Enhance US-CERT capabilities for control systems cyber security

Our control systems activities support NCSD's overall efforts to address cyber security across critical infrastructure sectors over the long term, as well as the US-CERT's capability in the management, response, and handling of incidents and vulnerabilities, and mitigation of threat actions specific to critical control systems functions. NCSD established the US-CERT Control Systems Security Center (CSSC) in partnership with Idaho National Laboratory (INL) and other Department of Energy (DOE) National Laboratories[3] in August, 2004. Through the use of Cooperative Research and Development Agreements (CRADA's) and other mutually benefiting agreements, the CSSC also incorporates partners from control systems industry associations, universities, vendors, and industry experts. The CSSC mission is to reduce the risk of cyber attacks on control systems, and as such, it provides facilities and expertise to support the reduction of risk in critical infrastructure through site and system assessments, demonstrations for education and awareness, risk assessment and risk analysis, adversarial awareness, and coordination among the national laboratories.

Through its partnerships and technological improvement efforts for systems and facilities, the CSSC has been maturing response capabilities to support US-CERT with control system expertise. The CSSC continues to work with the US-CERT in enhancing their ability to provide initial control system guidance and expertise, and a CSSC limited access secure portal (https://us-cert.esportals.net/) has been established for information coordination and dissemination of cyber threat and vulnerability alerts. A web site is under development to share control systems security information with our cyber security partners and the control systems community. The web site, which will be available in FY06, will also provide information, resources, and links for owners and operators to effectively defend their control systems. A "Tier II" support function will further support US-CERT by leveraging CSSC partners in incident response and vulnerability handling, and performing in-depth evaluation of specific attacks or exploits and determining the impact on various operating systems, components, and vendor systems.

[3] Pacific Northwest, Los Alamos, Argonne, Sandia, Lawrence Livermore and Savannah River

In FY06, CSSC will explore the need for establishing a trusted third-party within academia to serve as a voluntary reporting center to encourage open communication among the private sector regarding emerging control system threats and exploits. As such, the CSSC is developing a control systems incident management support tool to enhance US-CERT cyber threat notification efforts. It is designed for use when a new vulnerability is detected and will enable the identification of critical infrastructure at greatest risk to an identified threat, thereby enabling the CSSC to rapidly notify the facilities at the greatest risk. Owners and operators can then implement protective measures as appropriate to reduce that risk and mitigate damage to their systems. It is important to note that the effectiveness of the tool is dependent on the acquisition of current owner/operator system data. NCSD continues to work with Sector Specific Agencies to obtain data from the various sectors necessary to utilize the tool and maximize its benefits.

Goal 2 – Reduce control system vulnerabilities in critical infrastructure

To reduce control system vulnerabilities in our critical infrastructure, CSSC developed a draft cyber security protection framework for identifying control systems security protection measures and comparing them against existing security standards. The cyber security protection framework, which is based on the Common Criteria and an Industrial Control System Security Protection Profile developed by the National Institute of Standards and Technology, supports NCSD's mission to reduce cyber security risk within control systems. The framework provides a systematic methodology for assessing the cyber security posture of control systems. It is designed to reduce the burden on owners and operators by providing them with a means to select protective measures that apply to their specific architecture and operating environment and reduce their respective risk.

Application of the framework methodology results in a risk-based set of security measures. Risk is defined by DHS as **Risk** = **Threat** x **Vulnerability** x **Consequence**. To calculate quantitative values for risk, one must define the system of interest, establish attack-defense-failure scenarios, and consider the consequences of a successful attack. Then, protection measures are identified to reduce risk. The overall goal is to provide a quantitative, traceable, and supportable value of risk.

As part of this framework, the CSSC also has capabilities at INL to perform vulnerability assessments of control systems. For example, the CSSC leverages the National SCADA Test Bed funded by DOE and operated in partnership with Sandia National Laboratories. Linkages with these test beds and assessment facilities provides the CSSC with incoming and outgoing data traffic and communication channels necessary for the replication of control systems (e.g., PCS, SCADA) and components. These testing capabilities also support quick mock-ups of control systems and/or components to evaluate existing threats, vulnerabilities, and incidents as they are reported to the US-CERT.

The CSSC utilizes a unique "plug and play" patching system that allows engineers to assess systems or components in an environment simulating the conditions found in industry to include multiple communication pathways and live incoming and outgoing control systems specific data traffic. This allows for in-depth assessments of control systems in a near true-to-life environment. The CSSC is working with commercial vendors and DOE to complete assessments of three different control systems to identify cyber vulnerabilities, reverse engineer exploits, and provide solutions to secure

vendor systems. A code-based analysis has also been conducted in cooperation with a vendor/manufacturer to identify possible vulnerabilities and recommendations to secure the system.

Our adversaries are developing tools to hack into and take over control systems, and we need greater collective awareness of those capabilities to understand specific threats to and vulnerabilities of our control systems. As such, CSSC tracks information on current control systems security trends and threats, review and assesses new vulnerabilities and exploits as they are discovered or reported, and conducts analysis to better understand adversarial tools and capabilities. The CSSC considers specific exploit assessment scenarios on control systems and "reverse engineers" exploits to provide solutions to industry before an exploit is made public.

The cyber security protection framework also leverages best practices from industry for securing control systems against cyber attacks and organizes them so the control systems community can identify specific solutions to their security vulnerabilities. As part of the framework, implementation tools, such as a "self-assessment tool," have also been developed to allow owners and operators of industrial control systems to perform on-site self-assessments against a database of categorized security requirements. Each security requirement is supported by recommendations for meeting the requirement and mitigating vulnerabilities within the architecture of that particular control system. As new vulnerabilities emerge and associated solutions are developed, the framework of security requirements will expand and new protection solutions will be made available to the control system community. The protection framework provides categorized and graded guidance, component by component, for improving cyber security of control systems.

The draft security protection framework and its associated implementation tools are ready for validation. NCSD will soon pilot the self-assessment tool with multiple infrastructure sectors and will assist selected control system owners and operators in using the tool at their sites. This effort will help owners and operators identify security vulnerabilities within their systems, recommend solutions for reducing the risk of successful cyber attacks, and prioritize risk reduction efforts. The pilot effort will also allow NCSD to validate and enhance the self-assessment tool for future, widespread roll-out across the control system community. NCSD is also working with PSD and other Sector Specific Agencies to ensure that concepts from the cyber security protection framework are integrated into risk and vulnerability assessments across the sectors. For example, NCSD is working closely with the American Society of Mechanical Engineers and PSD to incorporate cyber into the Risk Analysis and Management for Critical Asset Protection (RAMCAP) framework.

Goal 3 - Bridge industry and governmental efforts through participation in working groups, standards development bodies, and user conferences

A primary objective of NCSD's Control Systems Security Program is to coordinate efforts among Federal, State, and local governments, as well as control system owners, operators, and vendors to improve control systems security within and across all critical infrastructure sectors.

In partnership with DHS' Science and Technology (S&T) Directorate, NCSD chairs the Process Control System Forum (PCSF). The PCSF includes industry, academia, and government representatives and is designed to accelerate the development of technology that will enhance the security, safety, and reliability of control systems, including legacy installations.

In addition to the PCSF, the CSSC works to enhance private sector awareness through participation in industry association meetings, user groups, and standards coordination work groups. For example, most recently, representatives from CSSC participated in a Railroad Association meeting in Annapolis, Maryland, the Pacific Northwest Economic Region 15th Summit, and the Interagency Forum for Infrastructure Protection in Portland, Washington. At all of these gatherings, attendees were provided with an overview of the CSSC program, capabilities, and with information on how they can participate and take advantage of what the CSSC program has to offer, including alert and informational bulletins, self-assessment and risk reduction calculation tools.

CSSC has also established relationships with a number of industry partners, including partnerships designed to facilitate initial assessments and develop risk reduction plans in various industry sectors. Our private industry partners provide experience in understanding vulnerabilities and operational perspectives, and bring established contacts within the control systems community. Specifically, they provide CSSC with control system expertise from various critical infrastructure sector perspectives; expertise and feedback on assessment tools; subject matter expertise regarding development of security requirements and best practices; assessment, research, and risk assessment capabilities; and contacts and opportunities to interface with sectors.

CSSC is also working with control system vendors to provide equipment for assessments to be conducted at CSSC facilities. They assist in identifying vulnerabilities based on their experience and work to resolve vulnerabilities in next generation and legacy systems as a result of assessments performed against their systems. A number of industries (e.g., oil and gas, chemical, petro-chemical, electrical, power generation plant automation [coal, hydro, and gas fired plants], and transportation) are contributing to these CSSC efforts to reduce cyber vulnerabilities in control systems. Partnerships with members of the control system community are designed to help NCSD better assist owners and operators secure their systems.

Goal 4 - Enhance control systems security awareness

The NCSD is engaged in several activities designed to increases awareness and provide the tools and products necessary to enable the critical infrastructures and key resources to secure their control systems against cyber threats. A key element is CSSC's awareness workshop program.

Our "threat-brief, demonstration, and mitigations" workshop has been well received by the control systems community. The first workshop was held in May, 2005 at a PCSF meeting in Dallas, Texas. Since then additional workshops have been held in Bellevue, Washington and Idaho Falls, Idaho. We anticipate that by late 2005, approximately eight workshops will have been conducted. The workshops include a brief overview of the threat picture, a cyber vulnerability demonstration, and a discussion of mitigation steps. NCSD has found that cyber vulnerability demonstrations are an effective method to show the impact that cyber attacks can have on their control systems and operations and that cyber security is essential to protect them.

Goal 5 - Make strategic recommendations for improvements to future generation secure control systems and security products

Cyber-related research and development (R&D) is vital to improving the resiliency of the Nation's critical infrastructures. This difficult strategic challenge requires a coordinated and focused effort from across the Federal Government, State and local governments, the private sector, and academia to advance the security of critical cyber systems.

Two components within DHS share responsibility for cyber R&D. The Science & Technology (S&T) Directorate serves as the primary agent responsible for executing cyber security R&D programs. NCSD has responsibility for developing requirements for cyber security R&D projects. NCSD supports the overall DHS R&D mission by identifying areas for cyber innovation and coordinating with S&T. NCSD collects, develops, and submits cyber security R&D requirements to provide input to the federal cyber security R&D community and specifically to inform the DHS S&T Directorate's cyber security research priorities. NCSD coordinates with S&T on the development of new technologies for securing SCADA systems and networks.

NCSD's Control Systems Security Program identifies R&D cyber security requirements for legacy and next generation control systems and security products through US-CERT CSSC operational activities such as incident management, site and system assessments, and analyses. As difficult problems which would benefit from advanced technological solutions are discovered, requirements are identified and forwarded to control systems vendors and DHS S&T for new R&D projects. Best practices, common vulnerabilities, and requirements for security standards are also shared with the control systems community to promote enhanced security for legacy and new control systems.

DHS S&T manages the Congressionally directed funding for the Institute for Information Infrastructure Protection (I3P). The I3P is a national research consortium composed of more than two dozen research entities, including academic institutions, non-profits, federally funded labs, and FFRDCs. In early 2005, the I3P launched a major initiative focused on addressing the vulnerabilities of SCADA systems in the oil and gas industry.

Moving Forward

NCSD has a robust effort underway to address the security of control systems through our Control Systems Security Program. The efforts of the CSSC toward realizing the five goals the Program sets forth, including the enhancement of capabilities, initiatives to reduce vulnerabilities, and establishment of partnerships, has moved the ball forward in this arena by increasing the control system communities' awareness of the need for control systems cyber security and providing them the tools and resources to secure their control systems.

Many activities are planned for the near future including:

- Developing and finalizing the CSSC portal and web site to enhance capabilities and encourage greater information exchange with the control system community.

- Supporting vulnerability assessments to determine the cyber security posture of legacy and next generation control systems at critical sites. Assessments will identify critical components threat vectors, and misconfigurations in hardware, applications, and network topologies within our current infrastructure and recommend protective measures. This information will aid in determining the level of compliance with current best practices and control system protection framework requirements.
- Continuing to integrate CSSC activities, skills, and capabilities to identify particular high risk cyber vulnerabilities. Specifically, for FY06 high-risk system vulnerabilities will be identified in at least two critical infrastructure sectors and then security enhancements to mitigate those vulnerabilities will be identified. Other site assessments will be supported as appropriate to identify cyber risks to control systems.
- Encouraging the voluntary implementation of security measures. The CSSC will accomplish this through development of a "Business Case," beginning in FY06. Development of a business case will demonstrate cost-benefit where the cost will be represented as the cost of implementing countermeasures and benefit will be the reduction of risk. Risk analysis is the basis for the business case.
- Continuing to work with PSD and other Sector Specific Agencies to integrate cyber security and control systems security efforts into risk and vulnerability assessment efforts such as Comprehensive Reviews, the Vulnerability Identification Self Assessment Tool, and the Risk Analysis and Management for Critical Asset Protection.
- Continuing to participate in forums and meetings to raise awareness while conducting targeted outreach activities in sectors and with senior executives to not only pilot and validate our control systems protection framework and tools but also to create an understanding among control system owners and operators of the need for and importance of security.

We are committed to achieving success in meeting our goals and objectives, but we cannot do it alone. We will continue to meet with industry representatives, our government counterparts, academia, and state and local representatives to formulate the partnerships needed for productive collaboration and leverage the efforts of all, so we, as a nation, are more secure in cyberspace and in our critical infrastructures.

Again, thank you for the opportunity to testify before you today. I would be happy to answer any questions you have.